binalyze!

Security Operations Center (SOC) Use Cases

Turbo-charge your SOC with
Investigation & Response Automation
powered by digital forensics

USE CASE 1

Lightning fast evidence collection at scale

X36 TIMES FASTER

- Replace traditional forensic solutions, that take days to complete for one asset, with ultra-fast & innovative investigation and response automation
- Do much more without onboarding additional hard to find talent, or overloading experienced SOC analysts
- Gain full forensic visibility and prevent blind spots from limited alert-level visibility provided by EDR/ XDR/SIEM

Simple and powerful

• 1-click evidence collection
• Integrated, automated, scheduled – you decide

Out-of-box support for 500+ evidence types + full disk

• Operating system artifacts, browser evidence, application logs
• Network packet capturing
• Image a disk to remote cloud repositories with a few clicks

Faster than traditional disk imaging methodology

• Evidence acquisitions take as little as 10 minutes from start to finish

Chain of custody made easy

• 6x faster, parallel evidence compression compared to traditional products
• Evidence hashing as standard
• Military grade AES-256 encryption

Widest platform coverage on the market

• Supports Windows, macOS, Linux,ESXi, Chromebook, Azure & AWS

Quickly pivot into investigations with case relevant information

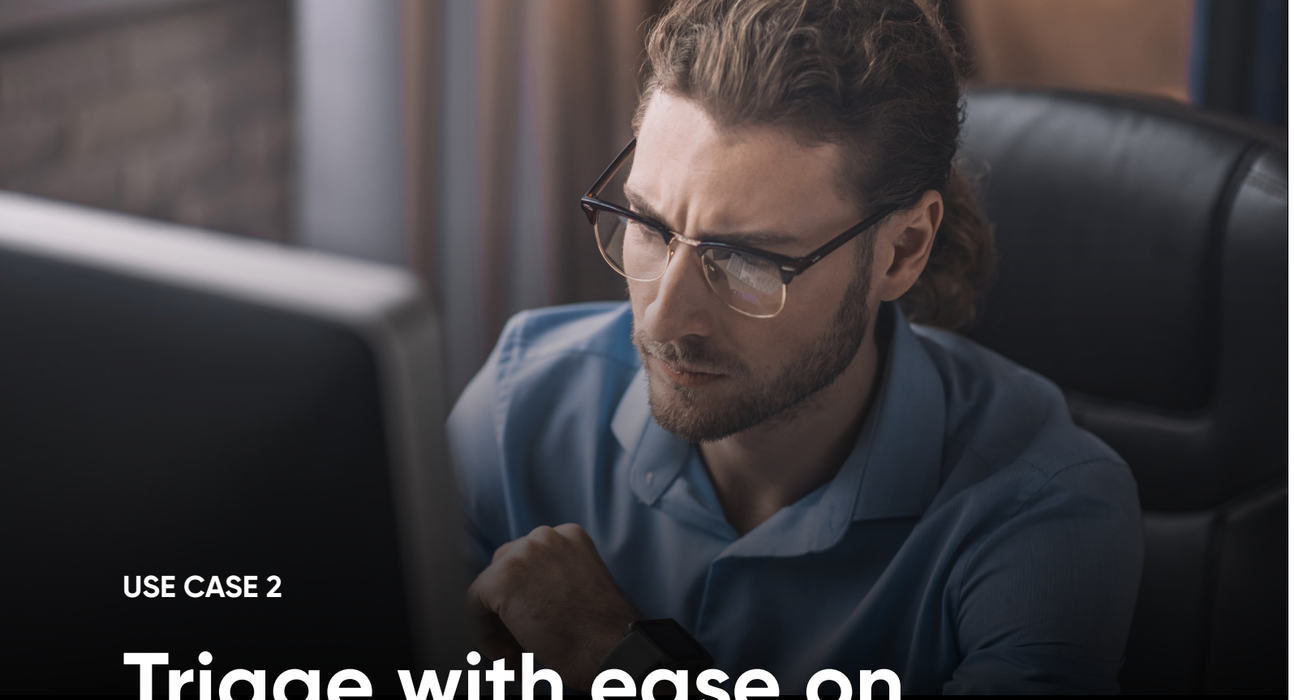
• Forget about running dozens of open source utilities and scripts
• Consolidated view of all the collected evidence in a single pane of glass

Runs smoothly on thousands of assets in parallel

• Battle tested globally on 100k asset enterprises

Automated timestamping

• Supports RFC-3161 timestamping for proof of existence and evidence integrity



USE CASE 2

Triage with ease on thousands of assets

Combine YARA, Sigma, osquery

- Automatically respond when an IoC is found, replacing manual and time consuming processes
- Decrease MTTR (mean time to respond) and MTTC (mean time to contain) by searching for what matters on thousands of assets in parallel
- Write IoC rules with an easy to use editor and use them on all platforms

All IoC formats in one platform

• Provides contextual YARA variables for lightning fast IoC scanning

• Use Sigma for searching inside event logs, right on the endpoints

• Unleash the power of osquery for triage at scale

Intuitive Visual Studio Code based online editor

• Operating system artifacts, browser evidence, application logs

• Network packet capturing

• Image a disk to remote cloud repositories with a few clicks

Powerful keyword searching across your case reports

• Text, RegEx, Wildcard pattern matching on parsed evidence, event logs, file names and browser history

Write once, match everywhere

• Hunt across file system, memory, event logs, and even in browser history with ease

• Supports Windows, Linux, macOS, IBM AIX

USE CASE 3

Automated compromise assessment

Intelligence-led updates

- Prevent SOC analyst burn-out by helping them prioritize what matters most in minutes
- Level up your SOC caseload capacity with automated evidence analysis and compromise assessments at scale
- See MITRE ATT&CK mappings to provide rapid understanding of malicious behaviors

Meet DRONE, your decision support system

• Evaluate evidence and assets using proprietary analyzers to highlight what matters most

• Runs generic IOC rules and automatically maps and displays findings in an easy to navigate MITRE ATT&CK Matrix

Complement your detection and monitoring solutions with forensic depth

• Designed to take a forensic approach, DRONE enables a holistic assessment in minutes

• Highlights webshells, ransomware traces, vulnerabilities, and much more automatically

Evaluate thousands of assets simultaneously without the noise

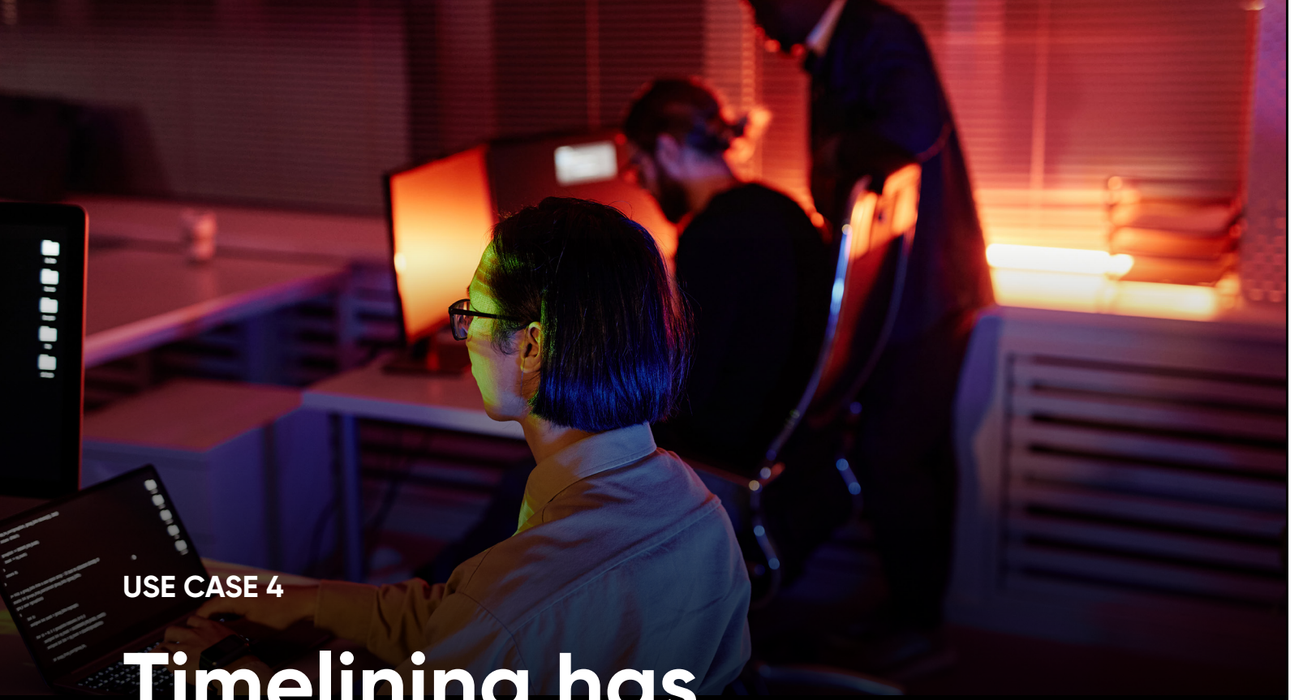
• Prioritize next steps with automatic assignment of ‘high’, ‘medium’, ‘low’, and ‘matched’ to findings

• Quickly search across insights with unified view of case-related findings in the Investigation Hub

Up-to-date integration of real-world intelligence

• Automated evidence analyzers continuously updated and improved by dedicated team of cybersecurity researchers and malware analysts

• Quickly assess for exploitation of latest zero-days and IOCs



USE CASE 4

Timelining has never been so easy

Ready in minutes

- Full forensics timeline without any storage and timeframe limitations. See all evidence starting from an asset's installation date.
- Web-based, ultra-fast & collaborative timeline experience, as if your SOC analysts are working in the same room
- Flags and filters to drill down on important events and speed up report creation understanding of malicious behaviors

1-click, collaborative timeline creation

• Select assets to create individual or super timelines

• Web based, ultra-fast timelining experience that can be viewed by all remote teammates

Easy to use event filters

• Designed to take a forensic approach, DRONE enables a holistic assessment in minutes

• Highlights webshells, ransomware traces, vulnerabilities, and much more automatically

Build timelines as your investigation develops

• Easily add a new asset to further add context to the timeline

• Enrich your timelines with CSVs in a format agnostic way - right from your browser

USE CASE 5

Compare forensic acquisitions in seconds

Ready in minutes

- Decreases the amount of evidence to look at to speed up the case closing time
- Unlock proactive digital forensics use cases for rapid assessment of your critical assets whether your EDR/XDR detects it or not
- Do much more without onboarding additional hard to find talent, or overloading experienced SOC analysts
- Capture forensic snapshot of your critical assets on a scheduled basis without worrying aboutstorage

An accessible approach to digital forensics

• Quickly see undetected changes including what, how and when

• Complements existing event monitoring and other traditional defensive security approaches

Schedule baseline acquisitions for your critical assets

• Enable a proactive security approach by continuously snapshotting your most critical assets

• Works even when your EDR/XDR is uninstalled/disabled by the attackers

Reduce the noise in your investigations

• No more searching for the needle in a haystack

• Look at what matters most with an intuitive comparison report with property level visibility

Enhanced Threat Hunting

• Turn the tables on stealthy attackers and use baseline analysis to unlock continuous assessment of your critical assets

• Covers significant areas of the system often used by attackers

USE CASE 6

Best in class, remote live shell that empowers your SOC

- Rapid response with cross-platform commands designed for Digital Forensics and Incident Response
- Retrieve any evidence from the asset quickly by eliminating time consuming internal communications with real-time live shell
- Upload your toolkit to the interACT Library for easy transfer and execution

Cross-platform, simple and powerful remote shell

• Use equivalent commands across Windows, Linux and macOS
• Write once, runs the same everywhere
• Supports auto-complete

Supports roles and privileges

• Control who can run what in your team for effective access control

• Three privilege levels (enumerate, read, write & execute) enables fine grained access to assets

Flexible and extendible command set

• Support full disk imaging, osquery and native shell access

• Run native commands such as the ‘exec’ command

interACT library

• Send and retrieve files between your browser and assets from a shared library

• Upload your toolkit and use them on the asset with a single ‘put’ command

Extensive logging and auditing

• See what is executed including the command results

• Integrates with your SIEM/ syslog for streaming command logs

binalyze!

headtechnology
it · security · distribution · services

Authorized Distributor

www.headtechnology.com

sales@headtechnology.com

Turbo-charge your SOC with Investigation and Response Automation powered by digital forensics

Binalyze is an innovator in Investigation and Response Automation. Binalyze's AIR platform empowers SOC teams to accelerate the time to close investigations without compromising on accuracy with end-to-end investigation capabilities and the powerful combination of forensic-level visibility, automation, and collaboration.

Find out more at www.binalyze.com